

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No. : 09/898,286 Confirmation No. 2215
Applicant : Geoffrey Donald Tremain
Filed : July 3, 2001
TC/A.U. : 2131
Examiner : Eleni A. Shiferaw
Docket No. : 1821-01100
Customer No.: 23505
Title: Method and Apparatus for Providing Computer Service

RESPONSE TO FINAL OFFICE ACTION DATED JULY 22, 2005
AND AMENDMENTS UNDER 37 CFR 1.116

Attorney Dkt. No.: 1821-01100
Date: January 20, 2006

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the Office Action dated July 22, 2005, please amend the above-identified application as follows:

The Claims are reflected in the listing of claims that begins on page 2 of this paper. There are currently no amendments.

Remarks/Arguments begin on page 12 of this paper.

The Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Previously presented) Apparatus providing one or more computer services for a plurality of customers, the apparatus comprising a real computer on which is set up at the request of each of said customers at least one virtual machine for each of said customers, said at least one virtual machine for each of said customers having a specification specified by and configurable by the respective customer and having an operating system running thereon.
2. (Original) Apparatus according to claim 1, wherein plural virtual machines are set up within the real computer for at least one of said customers.
3. (Original) Apparatus according to claim 1, wherein the or each virtual machine for at least one of said customers is connected to a virtual network set up for said at least one customer within the real computer.
4. (Original) Apparatus according to claim 3, comprising a virtual intrusion detection device for detecting an attack on the virtual network.
5. (Original) Apparatus according to claim 1, wherein at least one virtual machine is connected to a virtual firewall that is connectable to an external network to which customers and/or other users can connect such that access to said at least one virtual machine by a customer or other user via a said external network can only take place through a virtual firewall.
6. (Original) Apparatus according to claim 1, wherein the or each virtual machine for a particular customer is connected to a virtual firewall that is dedicated to that customer's virtual machine or machines, each virtual firewall being connectable to an external network to which each of said customers and/or other users can connect such that access to a virtual machine by a

customer or other user via a said external network can only take place through a virtual firewall provided for that virtual machine or machines.

7. (Original) Apparatus according to claim 6, wherein each virtual firewall is set up within the real computer, the or each virtual machine for each customer being connected to a first port of the virtual firewall that is dedicated to that customer's virtual machine or machines, each virtual firewall having a second port connected to a virtual network that is set up within the real computer and that is connectable to an external network.

8. (Original) Apparatus according to claim 7, wherein the second port of each virtual firewall is connected to the same virtual network that is set up within the real computer and that is connectable to an external network.

9. (Original) Apparatus according to claim 5, wherein the or at least one of the virtual firewalls is implemented by a virtual machine on the real computer, said virtual firewall virtual machine running firewall software.

10. (Original) Apparatus according to claim 1, comprising a plurality of real data storage devices and at least one virtual storage subsystem that is configured to allow said real data storage devices to emulate one or more virtual storage devices.

11. (Original) Apparatus according to claim 10, wherein the at least one virtual storage subsystem is configured to emulate at least one respective virtual storage device for each customer.

12. (Original) Apparatus according to claim 10, comprising a detection device for detecting evidence of malicious software or hostile attack signatures on the at least one virtual storage subsystem.

13. (Original) Apparatus according to claim 1, wherein the apparatus is configurable to provide at least one of the services selected from: file, data and archiving services; applications hosting services; database hosting services; data warehouse services; knowledge management

hosting services; digital media production services; "intellectual property" and streaming media services; simple web hosting services; complex e-Commerce web hosting services; high performance computation services; electronic messaging and conferencing services; and, learning neuro-computer services.

14. (Original) Apparatus according to claim 1, comprising virtual private network software to provide an encrypted communication channel for communication between at least some of said virtual machines.

15. (Original) Apparatus according claim 1, comprising virtual private network software to provide an encrypted communication channel for communication between at least one virtual machine and an external computer.

16. (Original) Apparatus according claim 1, comprising virtual private network software to provide an encrypted communication channel for communication between a first virtual network and a second virtual network.

17. (Original) Apparatus according to claim 1, comprising virtual private network software to provide an encrypted communication channel for communication between a virtual network and an external computer.

18. (Original) Apparatus according claim 1, wherein the real computer comprises plural physical computers.

19. (Original) In combination, a first apparatus according to claim 1 and a second apparatus that is substantially identical to said first apparatus, the first and second apparatus being connected by a communications channel so that the second apparatus can provide for redundancy of the first apparatus thereby to provide for disaster recovery if the first apparatus fails.

20. (Previously presented) A method of providing one or more computer services for a plurality of customers, the method comprising the steps of:

a service provider setting up on a real computer at the request of each of said customers at least one virtual machine for each of said customers, said at least one virtual machine for each of said customers having a specification specified by and configurable by the respective customer and having an operating system running thereon.

21. (Original) A method according to claim 20, comprising the step of setting up plural virtual machines within the real computer for at least one of said customers.

22. (Original) A method according to claim 20, comprising the steps of setting up a virtual network for at least one of said customers within the real computer, and connecting the or each virtual machine for said at least one customer to said virtual network.

23. (Original) A method according to claim 22, comprising the step of using a virtual intrusion detection device for detecting an attack on the virtual network.

24. (Original) A method according to claim 20, comprising the steps of connecting at least one virtual machine to a virtual firewall, and connecting the or each virtual firewall to an external network to which customers and/or other users can connect such that access to a virtual machine by a customer or other user via a said external network can only take place through a virtual firewall.

25. (Original) A method according to claim 20, comprising the step of connecting the or each virtual machine for a particular customer to a virtual firewall that is dedicated to that customer's virtual machine or machines, and connecting each virtual firewall to an external network to which each of said customers and/or other users can connect such that access to a virtual machine by a customer or other user via a said external network can only take place through a virtual firewall provided for that virtual machine or machines.

26. (Original) A method according to claim 25, wherein each virtual firewall is set up within the real computer, the or each virtual machine for each customer being connected to a first port of the virtual firewall that is dedicated to that customer's virtual machine or machines, each virtual

firewall having a second port connected to a virtual network that is set up within the real computer and that is connected to an external network.

27. (Original) A method according to claim 26, wherein the second port of each virtual firewall is connected to the same virtual network that is set up within the real computer and that is connectable to an external network.

28. (Original) A method according to claim 20, comprising the step of configuring at least one virtual storage subsystem to allow multiple real data storage devices to emulate one or more virtual storage devices.

29. (Original) A method according to claim 28, comprising the step of configuring the at least one virtual storage subsystem to emulate at least one respective virtual storage device for each customer.

30. (Original) A method according to claim 28, comprising the step of using a detection device for detecting evidence of malicious software or hostile attack signatures on the at least one virtual storage subsystem.

31. (Original) A method according to claim 20, wherein the services provided include at least one of the services selected from: file, data and archiving services; applications hosting services; database hosting services; data warehouse services; knowledge management hosting services; digital media production services; "intellectual property" and streaming media services; simple web hosting services; complex e-Commerce web hosting services; high performance computation services; electronic messaging and conferencing services; and, learning neuro-computer services.

32. (Original) A method according to claim 20, comprising the step of using virtual private network software to provide an encrypted communication channel for communication between at least some of said virtual machines.

33. (Original) A method according to claim 20, comprising the step of using virtual private network software to provide an encrypted communication channel for communication between at least one virtual machine and an external computer.

34. (Original) A method according to claim 20, comprising the step of using virtual private network software to provide an encrypted communication channel for communication between a first virtual network and a second virtual network.

35. (Original) A method according to claim 20, comprising the step of using virtual private network software to provide an encrypted communication channel for communication between a virtual network and an external computer.

36. (Original) A method according to claim 20, comprising the step of moving said at least one virtual machine from a first real computer to a second real computer.

37. (Previously presented) A method of operating a real computer on behalf of plural customers, the method comprising the step of:

operating plural virtual machines on the real computer, each of said plural virtual machines having a specification specified by and configurable by a respective one of the customers in accordance with a computer service to be provided by the virtual machine on behalf of that customer, each of said virtual machines having an operating system running thereon.

38. (Original) A method according to claim 37, comprising the step of operating plural virtual machines within the real computer for at least one of said customers.

39. (Original) A method according to claim 37, comprising the step of operating a virtual network for at least one of said customers within the real computer, the or each virtual machine for said at least one customer being connected to said virtual network.

40. (Original) A method according to claim 39, comprising the step of using a virtual intrusion detection device for detecting an attack on the virtual network.

41. (Original) A method according to claim 37, wherein at least one virtual machine is connected to a virtual firewall, the or each virtual firewall being connected to an external network to which customers and/or other users can connect such that access to a virtual machine by a customer or other user via a said external network can only take place through a virtual firewall.

42. (Original) A method according to claim 37, wherein the or each virtual machine for a particular customer is connected to a virtual firewall that is dedicated to that customer's virtual machine or machines, each virtual firewall being connected to an external network to which each of said customers and/or other users can connect such that access to a virtual machine by a customer or other user via a said external network can only take place through a virtual firewall provided for that virtual machine or machines.

43. (Original) A method according to claim 42, wherein each virtual firewall is set up within the real computer, the or each virtual machine for each customer being connected to a first port of the virtual firewall that is dedicated to that customer's virtual machine or machines, each virtual firewall having a second port connected to a virtual network that is set up within the real computer and that is connected to an external network.

44. (Original) A method according to claim 43, wherein the second port of each virtual firewall is connected to the same virtual network that is set up within the real computer and that is connectable to an external network.

45. (Original) A method according to claim 37, wherein at least one virtual storage subsystem is provided and configured to allow multiple real data storage devices to emulate one or more virtual storage devices.

46. (Original) A method according to claim 45, wherein the at least one virtual storage subsystem is configured to emulate at least one respective virtual storage device for each customer.

47. (Original) A method according to claim 45, wherein a detection device is used for detecting evidence of malicious software or hostile attack signatures on the at least one virtual storage subsystem.

48. (Original) A method according to claim 37, wherein the services provided include at least one of the services selected from: file, data and archiving services; applications hosting services; database hosting services; data warehouse services; knowledge management hosting services; digital media production services; "intellectual property" and streaming media services; simple web hosting services; complex e-Commerce web hosting services; high performance computation services; electronic messaging and conferencing services; and, learning neuro-computer services.

49. (Original) A method according to claim 37, comprising the step of using virtual private network software to provide an encrypted communication channel for communication between at least some of said virtual machines.

50. (Original) A method according to claim 37, comprising the step of using virtual private network software to provide an encrypted communication channel for communication between at least one virtual machine and an external computer.

51. (Original) A method according to claim 37, comprising the step of using virtual private network software to provide an encrypted communication channel for communication between a first virtual network and a second virtual network.

52. (Original) A method according to claim 37, comprising the step of using virtual private network software to provide an encrypted communication channel for communication between a virtual network and an external computer.

53. (Currently amended) A method according to claim 37, comprising the step of moving said at least one virtual machine from a first real computer to a second real computer.

54. (Previously presented) A method of providing for a plurality of customers one or more computer services selected from: file, data and archiving services; applications hosting services; database hosting services; data warehouse services; knowledge management hosting services; digital media production services; "intellectual property" and streaming media services; simple web hosting services; complex e-Commerce web hosting services; high performance computation services; electronic messaging and conferencing services; and, learning neuro-computer services; the method comprising the steps of:

setting up on a real computer at the request of each of said customers at least one virtual machine for each of said customers, said at least one virtual machine for each of said customers having a specification determined in accordance with the computer service or services requested by said customer and being configurable by said customer, said at least one virtual machine having an operating system running thereon.

55. (Original) A method according to claim 54, comprising the step of moving said at least one virtual machine from a first real computer to a second real computer.

56. (Previously presented) Apparatus according to claim 1, wherein at least one of said virtual machines provides at least a virtual central processor unit.

57. (Previously presented) Apparatus according to claim 1, wherein at least one of said virtual machines is created using a virtual machine abstraction program.

58. (Previously presented) Apparatus according to claim 1, wherein at least one of said virtual machines is created using machine simulation/emulation software.

59. (Previously presented) A method according to claim 20, wherein at least one of said virtual machines provides at least a virtual central processor unit.

60. (Previously presented) A method according to claim 20, wherein at least one of said virtual machines is created using a virtual machine abstraction program.

61. (Previously presented) A method according to claim 20, wherein at least one of said virtual machines is created using machine simulation/emulation software.
62. (Previously presented) A method according to claim 37, wherein at least one of said virtual machines provides at least a virtual central processor unit.
63. (Previously presented) A method according to claim 37, wherein at least one of said virtual machines is created using a virtual machine abstraction program.
64. (Previously presented) A method according to claim 37, wherein at least one of said virtual machines is created using machine simulation/emulation software.

REMARKS/ARGUMENTS

Applicant acknowledges receipt of the Office Action dated July 22, 2005, in which the Examiner maintained the rejection of claims 1-3, 10-11, 13, 18-22, 28-29, 31, 36-39, 45-46, 48 and 53-55 as obvious over Bugnion (US 6075938) in view of Derks (US 6810033 B2); maintained the rejection of claims 4-9, 12, 14-17, 23-27, 30, 32-35, 40-44, 47 and 49-52 as obvious over Bugnion (US 6075938) in view of Derks (US 6810033 B2) in combination with Bowman-Amuah (US 6697824), and added a rejection of claims 37-39, 45-46, 48, 53 and 62-64 as anticipated under § 102(e) by Devine (US 6397242 B1).

Applicant again thanks the Examiner for her thoroughness in preparing the Office Action. At the same time, Applicant respectfully submits that the rejections of the present claims must fail for the reasons set out below.

Status of the Claims

Claims 1-64 are pending. All claims are rejected

Rejections under 35 U.S.C. § 103(a)

In support of her rejection of claims 1-3, 10-11, 13, 18-22, 28-29, 31, 36-39, 45-46, 48 and 53-55 as obvious over Bugnion in view of Derks, the Examiner asserts that Bugnion teaches “a combination of innovative emulation of the Direct Memory Access engine and standard distributed file system protocols to support a global buffer catch that is transparently shared across all virtual machines. . . operating system allows applications to explicitly share memory region across virtual machine boundaries and server contains interface to setup these shared regions to allow processes running on multiple virtual machines to share memory. . . and the at least one virtual machine for each of said customers having a specification specified by the respective customer.”

Applicant very respectfully points out that the passages cited by the Examiner in support of her assertion that Bugnion teaches the present invention, *i.e.* col. 5, lines 1-13 and col. 8, lines 56-66, simply do not support the Examiner's position. The cited lines read:

The approach of the present invention offers two different possible solutions to handle applications whose resource needs exceed the scalability of commodity operating systems. First, a relatively simple change to the commodity operating system can allow applications to explicitly share [sic] memory regions across virtual machine boundaries. The monitor contains a simple interface to setup these shared regions. The operating system is extended with a special virtual memory segment driver to allow processes running on multiple virtual machines to share memory. For example, a parallel database server could put its buffer cache in such a

shared memory region and have query engines running on multiple virtual machines.

FIG. 1 shows how the virtual machine monitor allows multiple copies of potentially different operating systems to coexist. In this figure, five virtual machines coexist on the multiprocessor. Some virtual machines run commodity uniprocessor or multiprocessor operating systems, and others run specialized operating systems fine-tuned for specific workloads. The virtual machine monitor schedules the virtual resources (processor and memory) of the virtual machines on the physical resources of the scalable multiprocessor.

Like the rest of the Bugnion disclosure, these passages do not contain any mention of a “customer,” “third party,” or other term that could be construed in the manner asserted by the Examiner, or of providing “computer services” for the “customers.”

Applicant again respectfully submits that the rejection over Bugnion is based on a fundamental misunderstanding as to what is claimed in the present application and what is disclosed in the cited art. Specifically, Bugnion discloses a virtual machine monitor that can be used to implement and supervise the operations of several virtual machines within a computer. Virtual machines, and the operation of virtual machines, are background art to both Bugnion and the present invention, having been known for several years. Bugnion’s virtual machine monitor operates to set up and supervise, or “monitor”, virtual machines within a computer, so as to enhance their operations.

However, Bugnion does not contemplate a system in which one or more virtual machine is set up for and by each of several customers to provide computer services for the customers. This concept of allowing multiple third parties to configure and control a plurality of virtual machines within a computer is entirely novel. As evidence of the novelty and non-obviousness of the presently claimed concepts, Applicants submit herewith an Affidavit of Geoffrey Donald Tremain, who is the inventor of the present case and an expert in the technology underlying this invention.

As set out in the Affidavit, until the present invention, virtual machines on a single computer were controlled by a single entity, often a single individual, and were typically used for diagnostic or comparative assessments of software (such as new applications or operating systems being developed by the individual). Neither Bugnion nor the other references discloses or suggests the use of plural virtual machines on a real computer *in which at least one virtual machine is set up*

by and for each of the customers, with each of those virtual machines having a specification that is specified by the respective customer.

As stated in the present specification, the problems solved by the present invention were significant and very real technical problems. At the time of the invention, entities who provided hosting services for multiple third parties (*i.e.* customers) either used multiple physical computers, with a respective real computer being dedicated to each customer, or resorted to a space-sharing system that did not allow the security and independence that are afforded by the present invention.

Despite the significant cost and maintenance implications for the provider, despite the need for a system that would avoid these problems, and despite the existence of virtual machines, until the present invention, no one had contemplated a system in accordance with the present invention. In the face of such a long-felt need, Applicants conception of the present invention is a patentable advance over the state of the art.

As discussed in the previous *Response* and in the enclosed Affidavit, Derks refers to “Private Virtual Networking”, which is more commonly known as “virtual private networking” or “VPN.” This technology relates solely to telephony and specifically to techniques for making a secure transmission channel over an insecure network. This has nothing whatsoever to do with virtual machine technology. Moreover, the examiner on page 3 of the office action of December 9, 2004 asserts that one having ordinary skill in the art at the time the invention was made would employ the teachings of Derks with the system of Bugnion because “it would allow to identify the gateway with the internet address carried by the set up request message and transmit data over the connection in order to address one out of more terminals connected to the remote gateway and set up a virtual connection.” However, this statement does not support the examiner’s position. Indeed, and again as set out in the enclosed Affidavit, it cannot be seen that this has any relevance to the present invention: the examiner’s references to “gateway”, “internet address”, “terminals connected to the remote gateway” and “virtual connection” make no sense in the context of the present invention, which relates to an innovative use of virtual machines to provide computer services to customers. Hence, the combination of Derks with Bugnion simply *does not support* the present obviousness rejection.

Rejections under 35 U.S.C. § 102(e)

In support of her rejection of claims 37-39, 45-46, 48, 53 and 62-64, the Examiner cites Devine. However, as discussed in the enclosed Affidavit, in terms of its relevance to the present

invention, Devine in essence discloses the same subject matter as Bugnion and is therefore equally irrelevant. In particular, as with Bugnion, Devine does not contemplate a system in which one or more virtual machine is set up for and by each of several customers to provide computer services for the customers. Hence, Devine does not anticipate claim 37, or claims 38, 39, 45, 46, 48, 53 and 62-64.

For all of the foregoing reasons, it is respectfully submitted that the invention of each independent claim is patentable. Because the rejection of the independent claims must fail, the rejection of claims 4-9, 12, 14-17, 23-27, 30, 32-35, 40-44, 47 and 49-52 as obvious over Bugnion in view of Derks in combination with Bowman-Amuah must also fail.

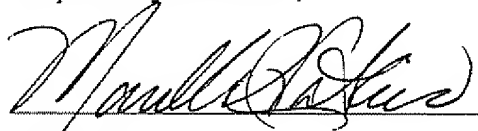
Affidavit

Applicant respectfully submits the attached Affidavit, which demonstrates why, in context of the state of the art to which this invention relates, the present claims describe a novel and non-obvious approach that was not contemplated by others. Indeed, others, when faced with the problems that are solved by the present invention, took burdensome and expensive steps because they did not have the benefit of the present concepts.

Conclusion

Applicant respectfully submits that the claims are in condition for allowance. If the Examiner has any questions or comments, or otherwise feels it would be advantageous, she is encouraged to telephone the undersigned at (713) 238-8043.

Respectfully submitted,



Marcella D. Watkins
Reg. No. 36,962
Conley, Rose P.C.
P. O. Box 3267
Houston, Texas 77253-3267
(713) 238-8000
ATTORNEY/AGENT FOR APPLICANT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Geoffrey Donald Tremain
App. Serial No.: 09/898,286
Group Art Unit: 2136
Filed: July 3, 2001
Examiner: Shiferaw, Eleni A
For: Method and Apparatus for Providing Computer Services

AFFIDAVIT OF GEOFFREY DONALD TREMAIN

Atty. Dkt. No.: 1821-01100

Date: January 19, 2006

Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450
Sir:

PURPOSE OF DECLARATION

This declaration is made in support of the *Response to Final Office Action Dated July 22 2005*, which is filed concurrently herewith

STATEMENT OF FACTS

- 1 I, Geoffrey Donald Tremain, state as follows:
- 2 I am over 18 years of age and competent to make this Affidavit;
- 3 I am employed by Ernst & Young Services Limited, a wholly owned subsidiary company of Ernst & Young LLP, the assignee of the above-identified pending patent application, and have been employed by them since November 1996 as an information systems and security consultant, with the current grade of Senior Manager;
- 4 I obtained a Bachelor of Science degree with honours in Physics from the University of Bristol, UK in 1986
- 5 I am the sole named inventor in the above-identified pending patent application;

6 In brief, the principal problem which is addressed by my invention as defined by the independent claims of the present application is how to host or provide computer services (such as applications hosting services, web hosting services, etc., as detailed in the present application) for plural customers in a secure way whilst minimizing the real physical resources which are required. This is a significant and very real and current technical problem.

7 At present, those who are providing such hosting services for third parties typically have very many real computers, with a respective real computer being dedicated to each customer. Before my invention, this was the accepted way of providing such services, being the most straightforward and obvious way to provide such services. This has significant cost and maintenance implications for the provider, which inevitably results in relatively high costs being passed onto the customers. Moreover, if customers run applications on a shared computer with a common operating environment, data and applications will be far less isolated from each other, raising security, functionality and performance difficulties.

8 The present invention solves this technical problem with a technical solution, namely the creation and use of plural virtual machines for the respective customers. The present invention delivers significant commercial advantages which include but are not limited to: lower costs of provisioning of service for the supplier, allowing higher profit margins as well as more competitive pricing to customers, and the ability to create, modify and terminate instantly and flexibly customer-specified and configured computing infrastructure on demand, in a way that provides strong isolation between different customers' systems, as well as strong isolation between systems of a single customer, for example when security isolation is desired between different parts of a system. In summary, the present invention gives customers the benefits of dedicated computer systems for the costs of shared ones, as well as giving them great flexibility in the speed with which they can procure, specify and configure their systems. Similarly, for the service provider, this provides a very competitive way of providing computer services to customers offering a mix of price, security isolation and flexibility benefits which cannot be achieved with conventional approaches.

9 At the date of filing of the present patent application, *and indeed generally today*, state-of-the-art approaches to provision of computer infrastructure by service providers to customers simply

did not and could not deliver these benefits, nor did they employ the present invention. Instead, as mentioned in paragraph 7 above, the state-of-the-art approaches either involved procurement, installation and configuration of dedicated infrastructure with resulting costs and considerable elapsed time, even though the customer's applications would not necessarily consume all available system capacity, or they involved use of shared systems which did not deliver the necessary degree of security isolation needed for the majority of business applications. Because of these limitations, most users of large-scale computer systems still choose to operate dedicated systems themselves, and are burdened with the necessary procurement, build and operating costs and elapsed time involved. Those skilled in the art of information systems infrastructure provision will recognize the potential of my invention to transform fundamentally the current global market in information technology infrastructure provision;

10 I have reviewed U.S. Patent No. 6,075,938 to Bugnion et al (hereinafter "Bugnion"), U.S. Patent No. 6,810,033 to Derks (hereinafter "Derks"), U.S. Patent No. 6,397,242 to Devine et al (hereinafter "Devine"), and U.S. Patent No. 6,697,824 to Bowman-Amuah (hereinafter "Bowman-Amuah"), which are cited against the present application:

11 The examiner asserts (section 8 of the OA) that the subject matter of independent claims 1, 20 and 54 is obvious in view of Bugnion and Derks:

12 In respect of claims 1 and 20, the examiner asserts (pages 12 and 13 of the OA) that Bugnion discloses "apparatus or a method providing one or more computer services for a plurality of customers, the apparatus comprising a real computer on which is set up of [*sic*] each of said customers at least one virtual machine for each of said customers, said at least one virtual machine for each of said customers having a specification specified by and configurable by the respective customer and having an operating system running thereon." [emphasis added]. However, based on my review of Bugnion, I can state that Bugnion does not make any reference to customers at all, and does not disclose providing one or more computer services for a plurality of customers, nor setting up a virtual machine for each of a plurality of customers, nor a virtual machine that has a specification that is specified by and configurable by a customer, nor the benefits of the application of such technology as described in paragraph 8 above;

13. The examiner further asserts (page 13 of the OA) that Bugnion does not explicitly teach "set up request of each of said customers [sic]". I can state that this is true, because Bugnion does not refer to customers at all, as stated above:

14. The examiner further asserts (page 13 of the OA) that Derks discloses "set up request of each of said customers to set up virtual connections". As I will explain further below, Derks does not disclose virtual machines at all, but instead relates (only) to private virtual networking of voice telephony, rather than computer service provision:

15. In respect of claim 54, the examiner asserts (pages 13 and 14 of the OA) that Bugnion discloses "a method of providing for a plurality of customers one or more computer services selected from: file, data and archiving services; applications hosting services; database hosting services; data warehouse services; knowledge management hosting services; digital media production services; "intellectual property" and streaming media services; simple web hosting services; complex e-commerce web hosting services; high performance computation services; electronic messaging and conferencing services; and, learning neuro-computer services; the method comprising the steps of: setting up on a real computer of [sic] each of said customers at least one virtual machine for each of said customers, said at least one virtual machine for each of said customers having a specification determined in accordance with the computer service, and being configurable by said consumer [sic], said at least one virtual machine having an operating system running thereon" [emphasis added]. However, as stated above, Bugnion does not disclose customers at all, and does not disclose providing one or more computer services for a plurality of customers, nor setting up a virtual machine for each of a plurality of customers, nor a virtual machine that has a specification that is specified by and configurable by a customer;

16. Bugnion discloses what is known as a "virtual machine monitor", i.e. a piece of software that is used to create and monitor virtual machines on a real computer. I am familiar with virtual machines and virtual machine monitors, including the actual product that is the subject of Bugnion. Virtual machines as such are old and well known. As mentioned on for example page 17 of the present application and at column 2, lines 36 onwards of Bugnion, IBM developed virtual machine technology in the late 1960s and early 1970s and therefore this technology as such has been in existence for a very long time. A simple definition of a virtual machine is "a self-contained operating environment that behaves as if it is a separate computer". A virtual machine is created

using software, such as a virtual machine monitor as disclosed by Bugnion, and in essence only exists temporarily in the memory of a real computer. In the sense used in the present application, a virtual machine is a practically self-contained operating environment that behaves as if it is a separate computer, separately of the real or physical computer on which the software that generates the virtual machine is run:

17 Virtual machines were created historically to allow computer scientists and the like to develop new software applications and operating systems safely. The computer scientists would typically create a virtual machine on a real machine and use the virtual machine to develop and test new software (such as operating systems and software applications). Plural virtual machines might be set up, with each running different versions of the software. The main advantage of using the virtual machine rather than the real computer was that if the software being developed caused problems to the operating system running on the virtual machine or to the virtual machine itself, then only the virtual machine would “crash”, and the underlying real computer would not be affected at all. Thus, computer scientists could safely develop new software without concern as to whether the new software might cause problems for the real computer. The inconvenience of a real computer crashing was and is a significant problem, owing to the delay in restarting the computer and the like and because of the possibility of serious and irrecoverable damage being caused to the real computer.

18 Thus, Bugnion is directed to and, in terms of its relevance to my invention, relates only to a virtual machine monitor that can efficiently create plural virtual machines on a real computer. A computer scientist or the like can use the virtual machine monitor of Bugnion (or, for that matter, any other virtual machine monitor) to create plural virtual machines on a real computer. The computer scientist can then for example run the Linux operating system on one of those virtual machines, Windows XP on another of those virtual machines, MS-DOS on another of those virtual machines, etc. The computer scientist can then run different software applications on those virtual machines, or different versions of the operating systems on those virtual machines, and develop and test those software applications or operating systems without any concern that a “crash” on one of those virtual machines might affect that software applications or operating systems running on the other virtual machines. In this respect, Bugnion merely discloses one piece of software which could be used as a tool in forming an actual commercial embodiment of my invention, but does not disclose my invention. To go from the virtual machine monitor for forming virtual machines as

disclosed by Bugnion to my invention, which makes commercial use of virtual machines that have a specification that is specified and configurable by a customer to provide computer services to the customers with a range of distinct commercial benefits, was not an obvious modification of the prior art:

19. On the other hand, Derks relates to what Derks calls "Private Virtual Networking", which in the Derks patent refers to the ability of a telephone network to switch and route telephone calls in a particular way:

20. As can be seen, therefore, a virtual machine is nothing like a Private Virtual Network and vice versa. The technologies and underlying concepts are entirely different, they are created using entirely different technologies, and they were originally designed and exist for entirely different purposes. Telephony Private Virtual Network technology is not related to the present invention and an understanding of telephony Private Virtual Networks would not bring one skilled in the art of virtual machines any closer to the present invention;

21. For these reasons, my invention as defined in claims 1, 20 and 54 is not obvious in view of Bugnion and Derks. Despite the state of the art with respect to virtual machines, until I conceived of the presently claimed system, in which computer services are provided for plural customers by using a real computer having plural virtual machines for the different customers, each customer specifying and configuring their own virtual machine, no-one had contemplated such a system because no-one had appreciated that virtual machines could be used in this manner:

22. The examiner objects (section 5 of the OA) that the subject matter of independent claim 37 is known from Devine. In particular, the examiner asserts (page 5 of the OA) that Devine teaches "a method of operating a real computer on behalf of a plurality of customers, the method comprising the step of: operating plural virtual machines on the real computer, each of said plural virtual machines having a specification specified by and configurable by a respective one of the customers in accordance with a computer service to be provided by the virtual machine on behalf of that customer, each of said virtual machines having an operating system running thereon." [emphasis added]. However, based on my review of Devine, I can state that Devine does not make any reference to customers at all, and does not disclose operating a real computer on behalf of a

plurality of customers, nor setting up plural virtual machines having a specification that is specified by and configurable by the customers:

23 I note that, in terms of its relevance to my invention, Devine in essence discloses the same concepts as Bugnion, namely a virtual machine monitor, and therefore my comments above in relation to Bugnion apply equally to Devine. I note that the three named inventors of Devine are the same three named inventors of Bugnion:

24 It may be that the examiner is for some reason equating the term "customer" as used in the present claims with "software application" or similar. However, there is no basis for this comparison and in no sense can a "customer" be equated with or be considered to be analogous to a "software application". Customers are, according to standard usage of the term, people or entities who buy a good or a service. Software applications installed by a computer scientist are not "customers". Furthermore, each of the independent claims of the present application requires that the virtual machine have a specification that is specified and configurable by the customer. To the best of my knowledge the software applications that run on the virtual machines disclosed in Bugnion and Devine do not and cannot specify or configure the specification of the virtual machine:

25 Alternatively or additionally, it may be that the examiner is for some reason equating the term "customer" as used in the present claims with a "computer scientist" or the like, who uses a virtual machine monitor to create virtual machines. However, there is no basis for this comparison and in no sense can "customer" as used in the claims of my patent application be equated with or be considered to be analogous to a "computer scientist" or the like. In Bugnion for example, as conventional with virtual machines, typically one person (a computer scientist) would set up plural virtual machines on a real computer for his own use, for example to run several operating systems, one within each virtual machine. In my invention, a person (such as a service provider) provides apparatus on which is set up plural virtual machines for the customers (i.e. for other people). I refer here to claim 20 of my patent application which specifically refers to a service provider setting up at least one virtual machine for each of said customers. Thus, Bugnion discloses only one person setting up virtual machines for his own use, whereas my invention is concerned with one person (a service provider) setting up virtual machines for other people (the customers):

26. In addition, each of the independent claims of the present application requires an apparatus or a method that provides computer services (such as applications hosting services, web hosting services, etc. as detailed in the present application and mentioned above) for customers, by using virtual machines. The references do not suggest such a thing. Bugnion for example only discloses using his virtual machine monitor to form plural virtual machines on which several copies of computer operating systems can be run, see for example the Summary of the Invention section at column 4, lines 6 to 50 of Bugnion. Bugnion does not disclose using virtual machines to provide computer services:

27. Further Affiant sayeth not.